KEY SHARING APPARATUS

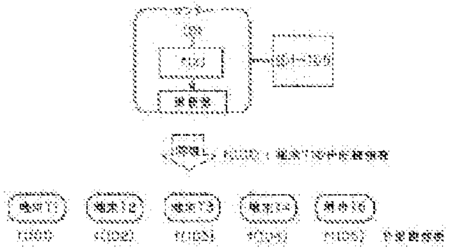
Publication number:	JP9212089 (A)
Publication date:	1997-08-15
Inventor(s):	MATSUZAKI NATSUME; TATEBAYASHI MAKOTO; HARADA TOSHIHARU; TOMABECHI AKITAKA; KANDA JUN +
Applicant(s):	MATSUSHITA ELECTRIC IND CO LTD +
Classification:	
- international:	***G09C1/00; H04L9/08;*** **G09C1/00; H04L9/08;** (IPC1-7): G09C1/00; H04L9/08
- European:	
Application number:	JP19960018541 19960205
Priority number(s):	JP19960018541 19960205

Also published as:

JP3620138 (B2)

Abstract of **JP 9212089 (A)**

PROBLEM TO BE SOLVED: To lessen the labor for cipher processing and to shorten business stop time until all the stations are updated by distributing the distribution key information of respective terminals to the respective terminals in such a manner that a secret key may be restored only when all of the distribution key information vary. SOLUTION: The respective terminals hold the different distribution key information. For example, the linear polynomial f(x)=ax+b mad (p) on a modulus (p) is considered with (p) as a prime number and (a), (b), (x) as remainder unknowns under the modulus (p). The (y) coordinates having the identification information of the respective terminals as an (x) coordinate value are set as the distribution key information of the respective terminals.; For example, only the T1 among the five terminals is expelled and the common secret key is shared by the remaining terminals. A center first determines the distribution key information of the terminal T1 to be expelled by inputting the identification information of the terminal T1 to the stored linear polynomial. The distribution key information of the terminal T1 determined in such a manner is transmitted by the same information to the respective terminals. The respective coeffts. of the corresponding linear polynomial, i.e., slant (a) and intercept (b), are determined from the two different coordinate points in a secret key calculation section.



Data supplied from the ***espacenet*** database — Worldwide